ITL FOCUSES ON DIGITAL FORENSICS

Digital investigators worldwide are benefiting from three digital forensic science projects in ITL's Software Diagnostics and Conformance Testing Division: the National Software Reference Library, the Computer Forensic Tool Testing project, and the Computer Forensic Reference Data Sets project. These projects promote the efficient and effective use of computer technology in the investigation of crimes involving computers. The U.S. Department of Justice's National Institute of Justice, federal, state, and local law enforcement, and NIST's Office of Law Enforcement Standards provide support for these projects. Resources are also contributed by numerous other sponsoring organizations from law enforcement, government, and industry.

The **National Software Reference Library (NSRL)** collects software from various sources and incorporates file profiles computed from this software into a Reference Data Set (RDS). Law enforcement, government, and industry organizations use the RDS to review files on a computer by matching file profiles in the RDS using an automated system. NSRL file data is typically used to eliminate known files, such as operating system and application files, during criminal forensic investigations. This reduces the number of files that must be manually examined and significantly increases the efficiency of the investigation. The majority of NSRL stakeholders are in federal, state and local law enforcement in the United States and internationally. Businesses and other government agencies also use the NSRL as part of their routine information technology operations. The Web site is http://www.nsrl.nist.gov/.

The **Computer Forensic Tool Testing (CFTT)** project provides a methodology for testing computer forensic software tools through the development of general tool specifications, test procedures, test criteria, test sets, and test hardware. ITL separates the activities of forensic investigations into discrete functions, such as hard disk write protection, disk imaging, string searching, etc. A test methodology is then developed for each category and made available on the web for toolmakers to test computer forensic tools. ITL reports its findings to the National Institute of Justice, which publishes test reports. In addition to forensic tools for acquisition and analysis of digital data on desktop and laptop computers, CFTT is also developing test methodologies for mobile devices. The Web site is http://www.cftt.nist.gov/.

The **Computer Forensic Reference Data Sets (CFReDS)** project provides documented sets of simulated digital evidence for examination by investigators. Since CFReDS has documented contents, such as target search strings seeded in known locations, investigators can compare the results of searches for the target strings with the known placement of the strings. Investigators can use CFReDS in several ways, including validating the software tools used in their investigations, checking out equipment, training investigators, and testing the proficiency of investigators as part of laboratory accreditation. The Web site is http://www.cfreds.nist.gov.

NISTIR 7490, *Digital Forensics at the National Institute of Standards and Technology*, by James R. Lyle, Douglas R. White, and Richard P. Ayers, describes these computer forensics projects in detail. Published in April 2008, the document is available at .

http://www.cftt.nist.gov/NISTIR_7490.pdf.

Patent Awarded for ITL's Refreshable Scanning Tactile Graphic Display

NIST was recently awarded U.S. Patent No. 7,352,356, "Refreshable Scanning Tactile Graphic Display for Localized Sensory Stimulation"; inventors are ITL's John Roberts, Information Access Division, and Nicholas Guttenberg, a former student in ITL. This invention enables devices allowing users to "view" text, Braille, and imagery using the sense of touch, both for accessibility for blind users, and for enhancing a virtual environment. Unlike haptic display, which uses force feedback to "push" against the user's muscles, tactile display makes use of the finely detailed, scanning sense of touch in the fingertips. Tactile display can be combined with haptics, for example, allowing a user both to squeeze a virtual orange and to feel its textured surface. Tactile display can be used for teleoperation (greatly improving the user's control of a robot built with a sense of touch), and even (with future miniaturization of components) to give detailed sense of touch to the gloves in an environment or pressure suit.

The user places a finger against a fingertip-sized display surface with hundreds of "stimulus points," typically round-tipped pins, which are set in a pattern that is rapidly updated as the user moves the finger and the display, creating the sensation that the finger is moving over a detailed surface matching the imagery in the controlling computer. The display can be mounted on a computer mouse or in the fingertips of a data glove.

NIST innovations include use of pressure or force-based touch stimulus rather than specified displacement of the pins, use of differential pressure to

2

convey tactile information, and use of human skin's natural elasticity to help control the pins. All of these are directed toward achieving a good match to the human sense of touch, and toward improving manufacturability and lowering cost.

ELIA Life Technology, Inc., of New York, N.Y., has licensed this technology for accessibility applications. The company has also licensed another NIST patent, No. 7,009,595, for a low-cost, two-dimensional tactile graphic display for accessibility.

NEW ITL PUBLICATIONS

Computer Security Incident Handling Guide
By Karen Scarfone, Tim Grance, and Kelly Masone

NIST Special Publication 800-61, Revision 1
March 2008
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

Computer security incident response has become an important component of IT programs. Security-related threats have become not only more numerous and diverse but also more damaging and disruptive. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. Topics covered include organizing a computer security incident response capability, handling incidents from initial preparation through the post-incident lessons learned phase, and handling specific types of incidents.

Guidelines on Active Content and Mobile Code
By Wayne A. Jansen, Theodore Winograd, and Karen Scarfone
NIST Special Publication 800-28, Version 2
March 2008
http://csrc.nist.gov/publications/nistpubs/800-28-ver2/SP800-28v2.pdf

This document provides an overview of active content and mobile code technologies in use today and offer insights for making informed IT security decisions on their application and treatment. The discussion gives details about the threats, technology risks, and safeguards for end user systems, such as desktops and laptops. Although various end user applications, such as email clients, can involve active content, Web browsers remain the primary vehicle for delivery and are underscored in the discussion. The tenets presented for

Web browsers apply equally well to other end user applications and can be inferred directly.

MINEX II Performance of Fingerprint Match-on-Card Algorithms – Phase II Report
By Patrick Grother, Wayne Salamon, Craig Watson, Michael Indovina, and Patricia Flanagan
NISTIR 7477
February 2008
http://fingerprint.nist.gov/minexII/minex_report.pdf

The MINEX II trial was conducted to evaluate the accuracy and speed of Match-on-Card verification algorithms. These run on ISO/IEC 7816 smart cards. They compare conformant reference and verification instances of the ISO/IEC 19794-2 COMPACT CARD fingerprint minutia standard. The test therefore represents an assessment of the core viability of the de facto leading compact biometric data element on the most mature personal identity credential. The result is relevant to users seeking to use minutia templates as an additional factor for authentication.

A Study of Users with Visual Disabilities and a Fingerprint Process
By Brian Stanton, Mary Theofanos, and Charles Sheppard
NISTIR 7484
February 2008
http://zing.ncsl.nist.gov/biousa/docs/NIST-IR%207484%20access_study.pdf

For the Department of Homeland Security United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program, the ITL Biometrics Usability group performed a usability test to study the interaction of people with disabilities with fingerprint devices. This report presents the results of a formative usability study that examined how persons with visual impairments interact with a fingerprint scanner. The

study was designed to investigate how those with a visual impairment can locate the scanning device, achieve proper placement of a hand on the device, and determine the duration of a fingerprint scan.

MARK YOUR CALENDAR

PIV PACS Integration Workshop
Date: May 1, 2008
Place: NIST, Gaithersburg, Maryland
Registration fee: $50
Sponsor: NIST

The purpose of this workshop is to exchange information on personal identity verification (PIV) integration in Physical Access Control Systems (PACS). NIST's Information Technology Laboratory wants to facilitate a discussion of draft NIST Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, and provide clarifications. Topics will include PACS, PIV, cardholder authentication, and Homeland Security Presidential Directive (HSPD) 12.

NIST technical contact: William MacGregor, 301/975-3883, william.macgregor@nist.gov
Conference website: http://www.nist.gov/public_affairs/confpage/080501b.htm

Workshop on 2D and 3D Content Representation, Analysis and Retrieval
Dates: May 1-2, 2008
Place: NIST, Gaithersburg, Maryland
Registration fee: none
Sponsors: System Integration for Manufacturing Applications Program, NIST Chemical Science Technology Laboratory; Information Discovery, Use, and Sharing Program, NIST Information Technology Laboratory

The 2nd Annual Workshop on 2D and 3D Content Representation, Analysis and Retrieval will bring together the various scientific research communities to present their recent research on image processing, image analysis, shape analysis, indexing, data mining, metadata, ontology, interoperability tools, benchmarks and evaluation methodologies. Topics include methods for storage, indexing, searching, recognition, clustering, retrieval, and exchange; benchmarks, comparative studies, evaluation methods and standards; bio-image processing and analysis; 3D shape analysis and recognition; data mining and pattern recognition methods in imaging; metadata, annotation, ontology, and semantic web; feature descriptors for images and 3D models, and retrieval systems for large distributed and heterogeneous databases.

NIST/ITL technical contact: Afzal Godil, 301/975-4262, afzal.godil@nist.gov
Conference website: http://www.itl.nist.gov/iad/vug/2dworkshop/

Applications of Pairing-Based Cryptography: Identity-Based Encryption (IBE) and Beyond
Dates: June 3-4, 2008
Place: NIST, Gaithersburg, Maryland
Registration fee: $145
Sponsor: NIST

This workshop will bring together security researchers from academia, government and industry to explore innovative and practical applications of pairing-based cryptography. Pairings have been used to create identity-based encryption schemes, but are also a useful tool for solving other cryptographic problems. In addition to presentations, the workshop will facilitate panel discussions among invited experts and workshop participants. Suggested topics for submissions in applications of pairing-based cryptography include Internet and web security; voting schemes; health care; access control schemes; IBE trust model; searching and processing encrypted data; broadcast systems; and novel security applications.

NIST technical contact: Andrew Regenscheide, 301/975-5155, andrew.regenscheide@nist.gov
Conference website: http://csrc.nist.gov/groups/ST/IBE/index.html

Mobile ID Workshop
Dates: June 4-5, 2008
Place: NIST, Gaithersburg, Maryland
Registration fee: $20
Sponsors: NIST and the FBI

The purpose of this workshop is to continue the development of a minimum set of operational requirements for enrollment, identification, and verification functions using Mobile ID devices. Comments on a draft document will be reviewed, discussed, and disposed. Topics will include levels of operation for capture and transmission of biometric data using mobile identification. Biometric types include fingerprint, face, and iris. The target audience is federal, state, and local government and law enforcement, biometric vendors, and consultants.

NIST technical contact: Elaine Newton, 301/975-2532, enewton@nist.gov
Conference website: http://fingerprint.nist.gov/mobileid/

Biometric Consortium Conference 2008 (BC2008)
Dates: September 23-25, 2008
Place: Tampa, Florida
Registration fee: $595/$695
Sponsors: NIST, NSA, DHS, Biometrics Task Force, NIJ, GSA, Volpe Center, AFCEA

This conference will focus on utilizing biometric-based solutions for a wide range of personal identification/authentication applications including homeland security and the prevention of identity theft. The target audience is policy developers and decision makers, government and industry executives, information technology (IT) users and developers, IT Chief Executive Officers, Chief Technical Officers and product managers, law enforcement officials, system integrators, personal authentication and information security specialists, educators and students, government, industry, and academia researchers. BC2008 will consist of presentations, seminars, and panel discussions with the participation of internationally recognized experts in biometric technologies, system and application developers, IT business strategists, and government and commercial officers.

NIST technical contact: Fernando Podio, 301/975-2947, fernando.podio@nist.gov
Conference website: http://www.biometrics.org/BC2008/index.htm